UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/538,954	03/31/2000	Carl M. Ellison	042390.P8107	9452

7590 06/29/2004

Thinh V Nguyen
Blakely Sokoloff Taylor & Zafman LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025

EXAMINER	
NORRIS, TREMAYNE M	

ART UNIT	PAPER NUMBER
2137	20

DATE MAILED: 06/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

7

7

Office Action Summary	Application No.	Applicant(s)	
	09/538,954	ELLISON ET AL.	
	Examiner	Art Unit	
	Tremayne M. Norris	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 March 2000*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,8,16 and 46-85* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,8,16,46-55,58-71 and 77-83* is/are rejected.

7)☒ Claim(s) *56,72-76,84 and 85* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 March 2000* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *14-17*.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments with respect to claims 1,8,16,48-85 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

2. Claim 8 objected to because of the following informalities: Claim 8 states "...address detector to detect physical addresses of transactions reference the isolated memory area.". It appears that the word "reference" should be changed to "referencing" or the word "that" should be placed in between "transactions" and "reference". Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1,8,16,46,51,52,55,57,58,63,64,66,68,69,71,80,81,83 are rejected under 35 U.S.C. 102(b) as being anticipated by Robinson et al (US pat 5,522,075).

Regarding claim 46, Robinson teaches a system comprising:

a processor that supports two or more operating modes (col.7 lines 20-21; col.7 lines 27-30; col.8 lines 13-14; col.13 lines 9-11) with different levels of privilege, including a ring 0 operating mode and a higher ring operating mode (col.4 lines 50-65);

a chipset communicatively coupled to the processor, wherein the chipset supports communication between the processor and a memory (col.7 lines 43-49);

configuration storage within the processor to store configuration parameters comprising:

a first configuration setting to define an isolated memory area within the memory; and

a second configuration setting to switch the processor between an isolated execution mode within the ring 0 operating mode and a non-isolated execution mode within the ring 0 operating mode (col.13 lines 53-55); and

an isolated execution circuit within the processor to generate isolated bus cycles when the processor executes in the isolated execution mode, wherein the isolated bus cycles enable a module to access a resource that is only accessible from the isolated execution mode of the ring 0 operating mode (col.13 line 53 thru col.14 line 11; isolated bus cycles are read/write or read/modify cycles).

Regarding claim 51, Robinson teaches the isolation execution circuit generates the logical processor access cycle in response to a transaction involving one of a logical processor entry to the isolated execution mode or a logical processor withdrawal from the isolated execution mode (col.13 line 53 thru col.14 line 11).

Regarding claim 52, Robinson teaches the isolated bus cycles generated by the isolated execution circuit comprise an isolated bus cycle that enables access to at least one resource selected from the group consisting of: the isolated memory area; an isolated register; and an isolated state (col.5 line 53 thru col.6 line 43).

Regarding claim 55, Robinson teaches a processor control register within the isolated execution circuit; and an execution mode word in the processor control register that is asserted when the processor is configured in the isolated execution mode (col.13 lines 53-55).

Regarding claim 57, Robinson teaches an access generator circuit in the isolated execution circuit and coupled to the configuration storage, the access generator circuit to generate an isolated access signal based on access information in a transaction and at least one of the configuration parameters, the isolated access signal being asserted when the processor is configured in the isolated execution mode, and

a bus cycle decoder in the isolated execution circuit and coupled to the access generator circuit, the bus cycle decoder to generate an isolated bus cycle corresponding to a destination in the transaction based on the access information and the asserted isolated access signal (col.13 line 53 thru col.14 line 11).

Claim 58 is substantially equivalent to claim 46, therefore claim 58 is rejected because of similar rationale.

Claim 1 is substantially equivalent to claim 57, therefore claim 1 is rejected because of similar rationale.

Regarding claim 8, Robinson teaches the configuration parameters comprise a memory setting to define an isolated memory area within memory external to the processor; and

the access generator circuit comprises an address detector to detect physical addresses of transactions reference the isolated memory area (col.10 lines 49-53).

Claims 63,64,68,69 are substantially equivalent to claims 51,52,8,55 respectively, therefore claims 63, 64,68,69 are rejected because of similar rationale.

Regarding claim 66, Robinson teaches the processor further comprises configuration storage to contain memory settings to define an isolated memory area in a memory external to the processor (col.13 lines 53-55).

Claim 71 is substantially equivalent to claim 46, therefore claim 71 is rejected because of similar rationale.

Claim 16 is substantially equivalent to claim 57, therefore claim 16 is rejected because of similar rationale.

Claims 80,81.83 are substantially equivalent to claims 51,52,55 respectively, therefore claims 80,81,83 are rejected because of similar rationale.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 47-50, 59-62,65,70,77-79 are rejected under 35 U.S.C. 103(a) as being unpatentable over Robinson et al, and further in view of Neufeld (US pat 5,668,971).

Regarding claim 47, Robinson teaches the system of claim 46 and isolated bus cycles generated by an isolated execution circuit, but does not teach bus cycles comprising: a data access cycle; a control access cycle; and a logical processor access cycle. Neufeld teaches bus cycles comprising: a data access cycle; a control access cycle; and a logical processor access cycle (col.16 lines 5-20). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Robinson's dual-mode protection ring system with Neufeld's system for controlling posted READ operations in order to prohibit access to protected memory address ranges (Neufeld col.4 lines 9-35).

Regarding claim 48, Robinson teaches the system of claim 46 and isolated bus cycles generated by an isolated execution circuit, but does not teach at least one bus cycle selected from the group consisting of: a data access cycle; a control access cycle; and a logical processor access cycle. Neufeld teache at least one bus cycle selected from the group consisting of: a data access cycle; a control access cycle; and a logical processor access cycle. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Robinson's dual-mode protection ring system with Neufeld's system for controlling posted READ operations in order to prohibit access to protected memory address ranges (Neufeld col.4 lines 9-35).

Regarding claim 49, Robinson and Neufeld teach the system of claim 48, in addition Neufeld teaches the execution circuit generates the data access cycle in response to a transaction involving a reference to the isolated memory area (col.15 line 66 thru col.16 line 20).

Regarding claim 50, Robinson and Neufeld teach the system of claim 48, in addition Neufeld teaches the execution circuit generates the control access cycle in response to a transaction involving an input/output reference to an register in a chipset external to the processor (col.11 lines 8-11; col.16 lines 5-20).

Claims 59-62 are substantially equivalent to claims 47-50 respectively, therefore claims 59-62 are rejected because of similar rationale.

Regarding claim 65, Robinson teaches the apparatus of claim 58 and an isolated execution circuit generating an isolated bus cycle, but does not teach generating bus cycles based on an access type and a destination transaction. Neufeld teaches generating bus cycles based on an access type and a destination transaction (col.15 line 66 thru col.16 line 20). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Robinson's dual-mode protection ring system with Neufeld's system for controlling posted READ operations in order to prohibit access to protected memory address ranges (Neufeld col.4 lines 9-35).

Regarding claim 70, Robinson teaches the apparatus of claim 58 and an isolated execution circuit generating an isolated bus cycle, but does not teach generating bus cycles based on an access type of a transaction. Neufeld teaches generating bus cycles based on an access type of a transaction (col.15 line 66 thru col.16 line 20). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Robinson's dual-mode protection ring system with Neufeld's system for controlling posted READ operations in order to prohibit access to protected memory address ranges (Neufeld col.4 lines 9-35).

Claims 77-79 are substantially equivalent to claims 48-50, therefore claims 77-79 are rejected because of similar rationale.

7. Claims 53,54,67,82 are rejected under 35 U.S.C. 103(a) as being unpatentable over Robinson et al, and further in view of Fujii et al (US pat 5,898,883).

Regarding claim 53, Robinson teaches the system of claim 46, but does not teach the first configuration setting to define the isolated memory area comprises at least one value selected from the group consisting of: a mask value; a base value; and a length value. Fujii teaches the first configuration setting to define the isolated memory area comprises at least one value selected from the group consisting of: a mask value;

a base value; and a length value (col.6 lines 42-48; col.10 lines 4-7; col.11 lines 10-20). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Robinson's dual-mode protection ring system with Fujii's memory access mechanism in order to increase the capacity of usable memory and to effectively utilize the address space without waste (Fujii col.2 lines 34-36).

Regarding claim 54, Robinson teaches the system of claim 46, in addition Fujii teaches the first configuration setting to define the isolated memory area comprises a mask value, a base value, and a length value (col.6 lines 42-48; col.10 lines 4-7; col.11 lines 10-20).

Claims 67 and 82 are substantially equivalent to claim 53, therefore claims 67 and 82 are rejected because of similar rationale.

Allowable Subject Matter

8. Claims 56,72-76,84,85 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. The following is a statement of reasons for the indication of allowable subject matter:

With respect to claim 56, the cited prior art fails to specifically teach the system of claim 46, further comprising a logical processor counter in the chipset that is updated in a first direction in response to a logical processor entry to the isolated execution mode and is updated in a second direction in response to a logical processor withdrawal from the isolated execution mode.

With respect to claim 72, the cited prior art fails to specifically teach the method of claim 71, further comprising: initializing the isolated execution mode, using a processor nub loader; loading a processor nub into the isolated memory area, using isolated bus cycles; and verifying an operating system nub, using the processor nub.

With respect to claim 73, the cited prior art fails to specifically teach the method of claim 72, further comprising: if the operating system nub verifies as good, loading the operating system nub into the isolated memory area, using isolated bus cycles.

With respect to claim 74, the cited prior art fails to specifically teach the method of claim 71, further comprising: loading a processor nub into the isolated memory area, using isolated bus cycles; loading an operating system nub into the isolated memory area, using isolated bus cycles; and generating platform verification data, based on attributes comprising: a platform key; the processor nub; and the operating system nub.

With respect to claim 75, the cited prior art fails to specifically teach the method of claim 74, further comprising: switching from the isolated execution mode to the non-isolated execution mode; and I loading an operating system kernel into non-isolated memory.

With respect to claim 76, the cited prior art fails to specifically teach the method of claim 75, further comprising: switching from the ring 0 operating mode to the higher ring operating mode; and executing an application in the higher ring operating mode.

With respect to claim 84, the cited prior art fails to specifically teach the method of claim 71, further comprising: in response to a logical processor entry to the isolated execution mode, updating a logical processor counter in a chipset in a first direction.

With respect to claim 85, the cited prior art fails to specifically teach the method of claim 84, further comprising: in response to a logical processor withdrawal from the isolated execution mode, updating the logical processor counter in the chipset in a second direction.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tremayne M. Norris whose telephone number is (703) 305-8045. The examiner can normally be reached on M-F 7:30AM-5:00PM alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703) 305-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Tremayne Norris

June 24, 2004

Matthew B. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137